



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/608,601	06/27/2003	Haixiang He	15918ROUS01U	2261

34645 7590 06/18/2007
JOHN C. GORECKI, ESQ.
P.O BOX 553
CARLISLE, MA 01741

EXAMINER

SMITHERS, MATTHEW

ART UNIT	PAPER NUMBER
----------	--------------

2137

MAIL DATE	DELIVERY MODE
-----------	---------------

06/18/2007

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/608,601

Applicant(s)

HE, HAIXIANG

Examiner

Matthew B. Smithers

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 04 April 2007.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-18 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1,2,4,7-16 and 18 is/are rejected.
- 7) ☒ Claim(s) 3,5,6 and 17 is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

Applicant's arguments, see amendment, filed April 4, 2007, with respect to the rejection(s) of claim(s) 1-7, 9-11 under 35 USC 103 have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of US 6,831,921 granted to Higgins.

The indicated allowability of claim 8 is withdrawn in view of the newly discovered reference(s) to US 6,831,921 granted to Higgins. Rejections based on the newly cited reference(s) follow.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1, 2, 4, and 7-11 are rejected under 35 U.S.C. 102(e) as being anticipated by US 6,831,921 granted to Higgins.

Regarding claim 1, Higgins meets the claimed limitations as follows:

Art Unit: 2137

"A method of establishing a VPN tunnel through a wireless network, the method comprising the steps of:

passing identifying information associated with a wireless user to a VPN host network;

evaluating the identifying information by the VPN host network to obtain a VPN host network access result;

and granting wireless access to the wireless user on the wireless network based on the VPN host network access result, to thereby enable both wireless network access and VPN host network access to be obtained without requiring evaluation of the identifying information by the wireless network." see column 5, line 27 to column 6, line 5; column 6, line 45 to column 7, line 24; column 8, lines 25-28 (In addition, the system can utilize the VPN which can encrypt the information . . . ensuring a higher level of security.); Figures 1, 2, and 3. (A customer is prompted to provide logon information to a VPN concentrator that will in turn authenticate the customer. Once the customer is authenticated a routable IP address is given to the customer for gaining access to the Internet. The wireless network does not authenticate any information only the VPN.)

Regarding claim 2, Higgins meets the claimed limitations as follows:

"The method of claim 1, wherein the step of evaluating comprises authenticating the wireless user based on the identifying information associated with the wireless user, and ascertaining whether the user is authorized to access at least one of the VPN host network and the wireless network." see column 5, line 27 to column 6, line 5; column 6, line 45 to column 7, line 24; column 8, lines 25-28 (In addition, the system can utilize the

VPN which can encrypt the information . . . ensuring a higher level of security.); Figures 1, 2, and 3.

Regarding claim 4, Higgins meets the claimed limitations as follows:

"The method of claim 1, wherein the step of passing identifying information to the VPN host network comprises receiving by the wireless network the identifying information, and transmitting by the wireless network at least a subset of the identifying information to the VPN host network." see column 5, line 27 to column 6, line 5; column 6, line 45 to column 7, line 24; column 8, lines 25-28 (In addition, the system can utilize the VPN which can encrypt the information . . . ensuring a higher level of security.); Figures 1, 2, and 3.

Regarding claim 7, Higgins meets the claimed limitations as follows:

"The method of claim 1, further comprising a step of establishing a VPN tunnel between the VPN host network and the wireless network." see column 5, line 27 to column 6, line 5; column 6, line 45 to column 7, line 24; column 8, lines 25-28 (In addition, the system can utilize the VPN which can encrypt the information . . . ensuring a higher level of security.); Figures 1, 2, and 3.

Regarding claim 8, Higgins meets the claimed limitations as follows:

"A method of establishing a VPN tunnel through a wireless network, the method comprising the steps of:

passing identifying information associated with a wireless user to a VPN host network;

evaluating the identifying information by the VPN host network to obtain an access result;

granting access to the wireless user on the wireless network based on the access result;

and establishing a VPN tunnel between the VPN host network and the wireless network;

wherein the wireless network includes a wireless access point, and wherein the VPN tunnel is established between the VPN host network and the wireless access point." see column 5, line 27 to column 6, line 5; column 6, line 45 to column 7, line 24; column 8, lines 25-28 (In addition, the system can utilize the VPN which can encrypt the information . . . ensuring a higher level of security.); Figures 1, 2, and 3.

Regarding claim 9, Higgins meets the claimed limitations as follows:

"The method of claim 1, further comprising assigning, by the VPN host network, an IP address for use by the wireless user." see column 5, line 27 to column 6, line 5; column 6, line 45 to column 7, line 24; column 8, lines 25-28 (In addition, the system can utilize the VPN which can encrypt the information . . . ensuring a higher level of security.); Figures 1, 2, and 3.

Regarding claim 10, Higgins meets the claimed limitations as follows:

"The method of claim 1, further comprising a step of enabling the wireless user to access an established VPN tunnel with the VPN host network." see column 5, line 27 to column 6, line 5; column 6, line 45 to column 7, line 24; column 8, lines 25-28

Art Unit: 2137

(In addition, the system can utilize the VPN which can encrypt the information . . . ensuring a higher level of security.); Figures 1, 2, and 3.

Regarding claim 11, Higgins meets the claimed limitations as follows:

“The method of claim 1, further comprising a step of establishing an encrypted session between the wireless user and the wireless network, and establishing a VPN tunnel between the wireless network and the VPN host network.” see column 5, line 27 to column 6, line 5; column 6, line 45 to column 7, line 24; column 8, lines 25-28 (In addition, the system can utilize the VPN which can encrypt the information . . . ensuring a higher level of security.); Figures 1, 2, and 3.

Claims 12-18 rejected under 35 U.S.C. 102(e) as being anticipated by US 20030079121 granted to Gilman et al.

Regarding claim 12, Gilman meets the claimed limitations as follows:

“A wireless access point, comprising:

a processor containing control logic configured to:

establish an encrypted session with a wireless user;

and establish a VPN tunnel to a VPN host network on behalf of the wireless user.” see paragraphs [0057]-[0061] and Figures 3, 4 and 5.

Regarding claim 13, Gilman meets the claimed limitations as follows:

“The wireless access point of claim 12, wherein the VPN tunnel to the VPN host network is an IP Sec tunnel, and wherein the encrypted session with the wireless user

Art Unit: 2137

comprises encrypting packets to be passed over the wireless network.” see paragraphs [0057]-[0061] and Figures 3, 4 and 5.

Regarding claim 14, Gilman meets the claimed limitations as follows:

“The wireless access point of claim 12, further comprising means for enabling the VPN host network to assign a private IP address to the wireless user.” see paragraphs [0057]-[0061] and Figures 3, 4 and 5.

Regarding claim 15, Gilman meets the claimed limitations as follows:

“The wireless access point of claim 12, a switch fabric configured to interface network ports and wireless access ports, and a routing information base configured to enable the control logic to route packets received at at least one of the network ports and wireless access ports to another of the network ports and wireless access ports.” see paragraphs [0057]-[0061] and Figures 3, 4 and 5.

Regarding claim 16, Gilman meets the claimed limitations as follows:

“The wireless access point of claim 12, wherein the wireless access point is an aggregation point.” see paragraphs [0057]-[0061] and Figures 3, 4 and 5.

Regarding claim 18, Gilman meets the claimed limitations as follows:

“The wireless access point of claim 12, wherein the control logic is configured to map traffic received over the wireless network from the wireless network user to the VPN tunnel.” see paragraphs [0057]-[0061] and Figures 3, 4 and 5.

Allowable Subject Matter

Claims 3, 5, 6, and 17 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

The following is a statement of reasons for the indication of allowable subject matter:

With respect to claim 3, the cited prior art fails to specifically teach wherein the identifying information comprises a conceptual ID, user ID and password.

With respect to claim 5 and 6, the cited prior art fails to specifically teach wherein the identifying information comprises at least a conceptual ID, user ID and password, and wherein the subset of the identifying information comprises the user ID and password.

With respect to claim 17, the cited prior art fails to specifically teach wherein the control logic is configured to rely on the VPN host network for authentication and authorization services with respect to the wireless user.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

A. Lor et al (US 20040068668) discloses a wireless local area network system.


B. Henry et al (US 7,174,456) discloses an authentication and access method for networking mobile devices.

Art Unit: 2137

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew B. Smithers whose telephone number is (571) 272-3876. The examiner can normally be reached on Monday-Friday (8:00-4:30) EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel L. Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.


Matthew B Smithers
Primary Examiner
Art Unit 2137